Wisconsin ServicePoint

SYSTEM ADMINISTRATION REQUIREMENTS

Policy:
HMIS staff will develop, implement and maintain specific components of operations of the web-based system. The staff will define the program, implement its standards, promote awareness of the system to all interested parties, and monitor the system's successes and failures to validate its effectiveness.

Standard:
Access to areas containing equipment, data, and software will be secured. All client identifying information will be strictly safeguarded. All data will be securely protected. Ongoing security assessments will be conducted on a regular basis.

Purpose:
To maintain security, performance and accuracy of HMIS-related data, software and equipment.

Supporting Documents:

Physical Security

HMIS is part of the State of Wisconsin Department of Commerce and is located at its headquarters in an 8-story office complex. Off-business hour security is provided. After normal business hours, card access is required and monitored. In addition, passwords are required to access individual workstations.

System Access Monitoring

ServicePoint™ automatically tracks and records access to every client record by use, date, and time of access. HMIS staff at Commerce will monitor access to system software. HMIS staff will regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access. HMIS staff will audit all unauthorized accesses and attempts to access information. Audit records shall be kept at least six months.

Media and Hardcopy Protection

Confidential data may be used for internal analysis or in the preliminary process of creating open data. Whenever confidential data is accessed:

- Hard copies shall be shredded when disposal is appropriate.
- Hard copies shall be stored in a secure environment such that is inaccessible to the general public or staff who do not require access. This may include the following: locked file drawers, in employee's physical possession and control like in a briefcase.
- Hard copies shall not be left out in the open or unattended.
- Electronic copies shall be stored only where the employee can access the data.
- Electronic copies shall be stored where a password is required to access the data if on shared server space.
- Electronic copies shall be stored in the employee's physical control like on a diskette, CD-ROM, or a personal computer accessed only by the employee.

User Authentication

The HMIS will only be accessed with a valid username and password

Resources:

HMIS WEB SITE (WISP)
https://wisconsin.servicept.com

HMIS INFOrmed
www.hmis.info/default.asp

Wisconsin HMIS
http://wisp.wi.gov

WISP HELP
sphelp@commerce.state.wi.us

Works in Progress:

combination, which is encrypted via SSL for Internet transmission to prevent theft. If an administrator enters an invalid password four consecutive times, the software automatically shuts them out of that session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Administration and System-wide Data

System Administrators will have full access to WISP, can add, edit and delete users, agencies, and programs and can reset passwords. Access to system-wide data will be granted based upon need, to access the data and with the approval of the steering committee. The number of staff with a System Administrator II designation will be limited to as few as possible. System Administrator will establish new agencies and agency administrators in the HMIS.

HMIS Administrator staff will not access an individual client's record with out express written or verbal consent of the agency administrator where the record is located or in order to create report where access is required for data quality or problem resolution.

Criminal Background Check

All system administrators must pass a criminal background check before they are given system administrator access.

Data Security

Wherever possible, all database access is controlled at the operating system and database connection level for additional security.

Client Record Disclosure

Information is not shared without appropriate client release. Clients have the right to know who has entered information and from what agency. The client has a right to know what information is contained in their records and what agencies have provided it.

Report Generation

Reports are completed in aggregate form without client identifiers.

Training[1]

HMIS training will be provided regularly throughout the year or as needed.